REMARKS

Applicant respectfully requests consideration of the subject application as amended herein. This Amendment is submitted in response to the Final Office Action mailed on October 28, 2008. Claims 1, 3-6, 8-13 and 15-25 are rejected. In this Amendment, claims 1, 4, 6, 9, 10, 13, 15 and 21 have been amended. New claim 29 has been added. No claims have been canceled. Therefore, claims 1, 3-6, 8-13, 15-25 and 29 are presented for examination.

Rejections Under 35 U.S.C. § 103

Claims 1, 3-6, 8-13 and 15-25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gehrmann et al. (US Pub. 2004/0176071, hereinafter "Gehrmann") in view of Ellison et al. (WO 01/75595, hereinafter "Ellison") and further in view of Le Saint et al. (US Pub. 2004/0218762, hereinafter, "Le Saint").

Claim 1 has been amended to recite:

> executing a protected application in a protected execution environment that is provided by a trusted platform, the protected execution environment being associated with a protected section of memory that is inaccessible to direct memory access and an unprotected section of memory that is accessible to direct memory access, wherein the trusted platform includes a trusted port mapped to the protected section of memory and an untrusted port mapped to the unprotected section of memory;
>
> determining, by the protected application, that information is to be accessed from a subscriber identity module (SIM) device that includes a SIM card, the SIM device being physically connected with the trusted platform;
>
> **exchanging unencrypted data that includes an encryption key between the SIM device and the protected application via a trusted path, the trusted path being a path through the trusted port, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted port;**
>
> encrypting additional data using the encryption key; and
>
> exchanging the encrypted data between the SIM device and the protected application via an untrusted path, the untrusted path being a path through the untrusted port.

(emphasis added).

The current Office Action states that the combination of Gehrmann and Ellison fails to teach exchanging unencrypted data that includes an encryption key between the SIM device and the application via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path. (Office Action, 10/28/08, page 5). Applicants agree that the combination of Gehrmann and Ellison fails to teach these limitations. However, the current Office Action cites Le Saint as teaching these limitations.

Le Saint teaches a system for securely exchanging information between a host computer system and a functionally connected cryptographic system. In Le Saint, secure communications are achieved by establishing an SSL-like communication pathway between the host computer system and the cryptographic system. (Le Saint, Abstract). Specifically, in Le Saint a security executive application on the host computer system encrypts a symmetric key using a public key, and sends the encrypted symmetric key to a cryptographic module over a path. (Le Saint, par. [0059]). The cryptographic module decrypts the encrypted symmetric key using a private key counterpart of the public key. (Le Saint, par. [0060]). Once both the security executive application and the cryptographic module have the symmetric key, further communications are encrypted with the symmetric key and sent over the same path used to send the symmetric key. (Le Saint, pars. [0064]). Le Saint does not teach sending the symmetric key over a first path and the messages encrypted using the symmetric key over a second path. In contrast, claim 1 recites, "exchanging unencrypted data … between the SIM device and the protected application via the trusted path," and "exchanging the encrypted data between the SIM device and the protected application via an untrusted path."

Additionally, in Le Saint, all communications are encrypted. The symmetric key is encrypted using asymmetric cryptography (e.g., a public key pair), and subsequent messages

are encrypted using symmetric cryptography. (Le Saint, pars. [0072]-[0073]). Le Saint does not teach exchanging unencrypted data that includes an encryption key. In contrast, claim 1 recites, "exchanging unencrypted data that includes an encryption key between the SIM device and the protected application via a trusted path."

Moreover, the symmetric key that is exchanged in Le Saint is protected using public key cryptography. The symmetric key is not protected via properties of a trusted port that connects the cryptographic module to the host computer system. In contrast, claim 1 recites, "wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted port."

For the above reasons, Le Saint fails to teach the features of claim 1 that are missing from Gehrmann and Ellison. Accordingly, Applicants respectfully submit that claim 1 and its dependent claims are patentable over the combination of Gehrmann, Ellison and Le Saint.

Claim 13 includes the limitations, "exchange unencrypted data that includes an encryption key with an application executed in the trusted environment via the trusted port, wherein the unencrypted data to be exchanged is secured from unauthorized access by the trusted port, and to exchange encrypted data with the application via the unprotected port." As noted above, the combination of Gehrmann, Ellison and Le Saint fails to teach or suggest such limitations. Accordingly, the applicants respectfully assert that the present invention as claimed in claim 13 and its corresponding dependent claims are patentable over the cited references.

Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) be withdrawn.

Conclusion

Applicant respectfully requests the withdrawal of the rejections and submits that pending claims 1, 3-6, 8-13, 15-25 and 29 are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicants' silence regarding any dependent claim is not to be interpreted as agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Benjamin Kimes at (408) 720-8300.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: January 28, 2009

/Benjamin A. Kimes/
Benjamin A. Kimes
Registration No. 50,870

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300